

Amendments to the Claims

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1-6. (cancelled without prejudice)

¹/₁. (previously amended) An encryption algorithm sharing management method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user and a user of the transmission side identifier indicating a user of a reception side; and querying a data base in which user identifiers indicating users, corresponding encryption algorithms and encryption keys thereof, are preliminarily described so as to obtain an encryption algorithm operated by the user of the transmission side and an encryption key thereof and an encryption algorithm operated by the user of the reception side and an encryption key thereof,

wherein if said encryption algorithm operated by the user of the transmission side is different from said encryption algorithm operated by the user of the reception side, signature data produced for the encryption key operated by the user of the transmission side is transmitted to the user of the transmission side and said encryption algorithm

operated by the user of the transmission side is encrypted with said encryption algorithm operated by the user of the reception side and are transmitted to the user of the reception side with signature data produced for the encryption key operated by the user of the reception side.

7. (previously amended) An encryption algorithm sharing management method for sharing the encryption algorithm for cryptographic communication, comprising the steps of:

8. from a user of a transmission side, obtaining a user identifier indicating the user of the transmission side and a user identifier indicating a user of a reception side; and querying a data base in which user identifiers indicating users, corresponding encryption algorithms and encryption keys thereof, are preliminarily described so as to obtain an encryption algorithm operated by the user of the transmission side and an encryption key thereof and an encryption algorithm operated by the user of the reception side and an encryption key thereof,

wherein if said encryption algorithm operated by the user of the transmission side is different from said encryption algorithm operated by the user of the reception side, signature data produced for the encryption key operated by the user of the transmission side is transmitted to the user of the transmission side and data indicating said encryption algorithm operated by the user of the transmission side and an encryption key produced based on the encryption key operated by the user of the reception side corresponding to a key length of said encryption algorithm operated by the user of the transmission side is encrypted with said encryption algorithm operated by the user of the reception side and

transmitted to the user of the reception side with signature data produced for the encryption key operated by the user of the reception side.

9 - 12. (cancelled without prejudice)

13. (previously amended) An encryption algorithm sharing management method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user of the transmission side and a user identifier indicating a user of a reception side; and querying a data base in which user identifiers indicating users, corresponding encryption algorithms and encryption keys thereof, are preliminarily described about each user so as to obtain an encryption algorithm operated by the user of the transmission side and an encryption key thereof and an encryption algorithm operated by the user of the reception side and an encryption key thereof,

wherein if said encryption algorithm operated by the user of the transmission side is different from said encryption algorithm operated by the user of the reception side, signature data produced for the encryption key operated by the user of the reception side is transmitted to the user of the reception side and said encryption algorithm operated by the user of the reception side is encrypted with said encryption algorithm operated by the user of the transmission side and transmitted to the user of the transmission side with the signature data produced for the encryption key operated by the user of the transmission side.

4
14. (previously amended) An encryption algorithm sharing management method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user of the transmission side and a user identifier indicating a user of a reception side; and
querying a data base in which user identifiers indicating users, corresponding encryption algorithms and encryption keys thereof, are preliminarily described about each user so as to obtain an encryption algorithm operated by the user of the transmission side and an encryption key thereof and an encryption algorithm operated by the user of the reception side and an encryption key thereof,

B 1
wherein if said encryption algorithm operated by the user of the transmission side is different from said encryption algorithm operated by the user of the reception side, signature data produced for the encryption key operated by the user of the reception side is transmitted to the user of the reception side and data indicating said encryption algorithm operated by the user of the reception side and an encryption key produced based on the encryption key operated by the user of the transmission side corresponding to a key length of said encryption algorithm operated by the user of the reception side is encrypted with said encryption algorithm operated by the user of the transmission side and transmitted to the user of the transmission side with signature data produced for to the encryption key operated by the user of the transmission side.

15 – 22 (cancelled without prejudice)